1-17. (Cancelled)

18. (New) A method for normalization of traffic data in a network comprising:

fragmenting and reassembling packets of said data;

dynamically establishing and maintaining a normalization table comprising said packets of said data;

simultaneously transferring said packets of said data to a network intrusion detection system and a monitored end-system; and

comparing said normalization table and identifiers of said packets of said data,

wherein said simultaneous transferring further comprises, when no inconsistencies are detected between said normalization table and identifiers of said packets of said data, said packets of said data are immediately forwarded contemporaneously to said network intrusion detection system and to said monitored end-system.

19. (New) The method according to claim 18, further comprising establishing information about said packet of said data without storing said data in said normalization table by extracting for each said identifier a header and calculating a length of said packet of said data, wherein said header indicates a length of said packet.

20. (New) The method according to claim 18, further comprising recording at least a partial receipt of said identifier by a sliding bit-mask which is moved to an offset, until said offset indicates receipt of all said data contained in said normalization table, wherein said receipt of said identifier is cleared after a time period which is selected equal or slightly higher than a lifetime of the last said packet inserted into said normalization table.

21. (New) The method according to one of the claims 18, wherein a distance and a path MTU to said monitored end system in a network are monitored by said network intrusion detection system are measured and stored in said normalization table before the receipt of said packet of said data by said monitored end-system.

22. (New) The method according to claim 18, further comprising retrieving from said normalization table TIME TO LIVE value for said packet of said data and measuring a path MTU for said monitored end-system,

wherein when a contents of said TIME TO LIVE value is lower than a predetermined value, then said TIME TO LIVE value replaces said predetermined value; and

wherein when said path MTU is lower than a size of the data packet a do not fragment FLAG is cleared.

23. (New) A method for normalization of traffic data in a network comprising:

fragmenting and reassembling packets of said data;

dynamically establishing and maintaining a normalization table comprising said packets;

simultaneously transferring said packets of said data to a network intrusion detection system and a monitored end-system; and

comparing said normalization table and identifiers of said packets of said data,

wherein said simultaneous transferring further comprises, when no inconsistencies are detected between said normalization table and identifiers of said packets of said data, said packets of said data are immediately forwarded contemporaneously to said network intrusion detection system and to said monitored end-system, and

wherein said dynamically establishing and monitoring comprises adding an aging bit to all entries in said normalization table, wherein said aging bit is set whenever said entries are retrieved from said normalization table.

24. (New) The method of claim 23, wherein said dynamically establishing and maintaining further comprises periodically sequentially resetting after a time period aging bits previously reset.

25. (Original) The method according to one of the claim 24, wherein said dynamically establishing and maintaining comprises periodically sequentially probing after a second time period, a distance and a path MTU to said monitored end-systems corresponding to said entries

stored in said normalization table and updating said normalization table when said distance and said path MTU have changed.

26. (New) The method according to claim 23, further comprising establishing information about said packet of said data without storing said data in said normalization table by extracting for each said identifier a header and calculating a length of said packet of said data, wherein said header indicates a length of said packet.

27. (New) The method according to claim 23, further comprising recording at least a partial receipt of said identifier by a sliding bit-mask which is moved to an offset, until said offset indicates receipt of all said data contained in said normalization table, wherein said receipt of said identifier is cleared after a time period which is selected equal or slightly higher than a lifetime of the last said packet inserted into said normalization table.

28. (New) The method according to one of the claim 23, wherein a distance and a path MTU to said monitored end system in a network are monitored by said network intrusion detection system are measured and stored in said normalization table before the receipt of said packet of said data by said monitored end-system.

29. (New) The method according to claim 23, further comprising retrieving from said normalization table TIME TO LIVE value for said packet of said data and measuring a path MTU for said monitored end-system,

wherein when a contents of said TIME TO LIVE value is lower than a predetermined value, then said TIME TO LIVE replaces said predetermined value; and

wherein when said path MTU is lower than a size of the data packet a do not fragment FLAG is cleared.

30. (New) A method for normalization of traffic data in a network comprising:

fragmenting and reassembling packets of said data;

dynamically establishing and maintaining a normalization table comprising said packets;

handling said packets of said data by any one of modifying said packets of said data, redirecting said packets of said data, and discarding said packets of said data.

simultaneously transferring said packets of said data to a network intrusion detection system and a monitored end-system; and

comparing said normalization table and identifiers of said packets of said data,

wherein said simultaneous transferring further comprises, when no inconsistencies are detected between said normalization table and identifiers of said packets of said data, said packets of said data are immediately forwarded contemporaneously to said network intrusion detection system and to said monitored end-system.

31. (New) The method according to claim 30, wherein said handling further comprises updating said normalization table by replacing an existing packet of said data in said normalization table with a current packet of said data when said existing packet of said data and said current packet of said data share the same said identifier.

32. (New) The method according to claim 30, wherein said handling further comprises updating said normalization table by inserting a new entry for a current packet of said data when no existing packet of said data comprises the same said identifier as said current packet of said data is found in said normalization table.

33. (New) The method according to claim 30, further comprising establishing information about said packet of said data without storing said data in said normalization table by extracting for each said identifier a header and calculating a length of said packet of said data, wherein said header indicates a length of said packet.

34. (New) The method according to claim 30, further comprising recording at least a partial receipt of said identifier by a sliding bit-mask which is moved to an offset, until said offset indicates receipt of all said data contained in said normalization table, wherein said receipt of

said identifier is cleared after a time period which is selected equal or slightly higher than a lifetime of the last said packet inserted into said normalization table.

35. (New) The method according to one of the claims 30, wherein a distance and a path MTU to said monitored end system in a network are monitored by said network intrusion detection system are measured and stored in said normalization table before the receipt of said packet of said data by said monitored end-system.

36. (New) The method according to claim 30, further comprising retrieving from said normalization table TIME TO LIVE value for said packet of said data and measuring a path MTU for said monitored end-system,

wherein when a contents of said TIME TO LIVE value is lower than a predetermined value, then said TIME TO LIVE value replaces said predetermined value; and

wherein when said path MTU is lower than a size of the data packet a do not fragment FLAG is cleared.

37. (New) A computer program product readable by machine, tangibly embodying a program of instructions executable by said machine to perform normalization of traffic data in a network, said method comprising:

fragmenting and reassembling packets of said data;

dynamically establishing and maintaining a normalization table comprising said packets;

simultaneously transferring said packets of said data to a network intrusion detection system and a monitored end-system;

comparing said normalization table and identifiers of said packets of said data,

wherein said simultaneous transferring further comprises, when no inconsistencies are detected between said normalization table and identifiers of said packets of said data, said packets of said data are immediately forwarded contemporaneously to said network intrusion detection system and to said monitored end-system, and

wherein, when inconsistencies are detected between said normalization table and said identifiers of said packets of said data, said packets of said data are handled by any one selected from modifying said packets of said data, redirecting said packets of said data, and discarding said packets of said data.

38. (New) The computer program product according to claim 37, wherein said handling further comprises updating said normalization table by inserting a new entry for a current packet of said data when no existing packet of said data comprising the same said identifier as said current packet of said data inserted in said normalization table.